Un grupo de investigadores en ciberseguridad del Instituto de Tecnología de Georgia y la Universidad Ruhr de Bochum ha identificado dos nuevos ataques de canal lateral que afectan al hardware de Apple, los cuales podrían emplearse para extraer información sensible de navegadores web como Safari y Google Chrome.

Estos ataques han sido nombrados SLAP (Data Speculation Attacks via Load Address Prediction on Apple Silicon) y FLOP (Breaking the Apple M3 CPU via False Load Output Predictions). Apple fue informada sobre estas vulnerabilidades en mayo y septiembre de 2024, respectivamente.

Al igual que la amenaza previamente revelada iLeakage, estas fallas están relacionadas con Spectre, un tipo de ataque que ocurre cuando la ejecución especulativa de una CPU genera errores, dejando rastros en la arquitectura interna del procesador y su caché.

La ejecución especulativa es un método de optimización que utilizan los procesadores modernos para anticiparse a la ejecución de instrucciones y mejorar el rendimiento.

Si la predicción falla, los cálculos resultantes de las instrucciones temporales se descartan y el estado del procesador vuelve a su estado previo.

Estos ataques se aprovechan de los rastros dejados por la ejecución especulativa, manipulando la CPU para inducir errores de predicción y forzar la ejecución de instrucciones transitorias. A pesar de que la CPU revierte estos cambios, los datos pueden ser inferidos a través de un canal lateral.

> *«En SLAP y FLOP, demostramos que las últimas CPUs de Apple no solo predicen el flujo de control de las instrucciones, sino también los datos con los que operará el procesador si estos no están disponibles de inmediato en la memoria»,* explicaron los expertos.
>
> *«A diferencia de Spectre, donde los errores de predicción afectan directamente las*

> *instrucciones ejecutadas, en este caso, la CPU ejecuta instrucciones correctas pero con datos equivocados. Sin embargo, mostramos que este comportamiento puede combinarse con técnicas avanzadas para ejecutar instrucciones incorrectas de manera intencionada.»*

SLAP, que compromete los procesadores M2, A15 y versiones posteriores, explota una función conocida como Load Address Predictor (LAP), un mecanismo en los chips de Apple que estima la próxima dirección de memoria que utilizará la CPU, basándose en patrones de acceso anteriores.

Si el LAP realiza una predicción errónea, la CPU puede realizar operaciones con datos fuera de los límites esperados bajo ejecución especulativa. Esto permite a un atacante recuperar información como correos electrónicos de usuarios autenticados o el historial de navegación en Safari.

Por otro lado, FLOP, que afecta a los procesadores M3, M4 y A17, explota un componente llamado Load Value Predictor (LVP), diseñado para mejorar el rendimiento adivinando el valor de los datos antes de que sean recuperados por el procesador.

Este ataque permite eludir verificaciones de seguridad en el manejo de memoria, exponiendo información confidencial. Los investigadores indican que FLOP podría utilizarse en Safari y Chrome para acceder a datos como historial de ubicaciones, eventos del calendario e incluso información de tarjetas de crédito.

Esta investigación se publica casi dos meses después de que expertos de la Universidad de Corea revelaran SysBumps, el primer ataque capaz de romper la aleatorización del espacio de direcciones del kernel (KASLR) en macOS para procesadores de Apple.

> *«Utilizando técnicas basadas en Spectre dentro de las llamadas al sistema, un atacante sin privilegios puede provocar traducciones de direcciones del kernel de su elección, generando cambios en la TLB en función de la validez de la dirección»*,

> explicaron Hyerean Jang, Taehun Kim y Youngjoo Shin. *«Esto posibilita un ataque que evade la protección de KASLR y compromete el aislamiento del kernel.»*

Además, otra investigación académica ha encontrado una forma de combinar múltiples canales laterales para superar las barreras en los ataques contra el núcleo del sistema operativo. Se ha descubierto que el etiquetado del espacio de direcciones, una técnica utilizada para mejorar la seguridad, en realidad introduce una nueva vulnerabilidad.

Este hallazgo ha llevado al desarrollo de un ataque práctico llamado TagBleed, que explota los buffers de traducción etiquetados (TLBs), utilizados para gestionar eficientemente la separación entre los espacios de memoria del usuario y del sistema. También se aprovecha de información residual de traducción para vulnerar KASLR, incluso en presencia de las mitigaciones más avanzadas.

> *«Esta filtración es suficiente para anular completamente la aleatorización del KASLR cuando se combina con otro canal lateral que utiliza el núcleo del sistema como intermediario para extraer datos adicionales sobre su ubicación en memoria»,* afirmó Jakob Koschel, investigador de VUSec.